Meridion Risk Assessment: USD Coin (USDC)

FIELD	VALUE
Digital Asset	USD Coin (USDC)
Risk Areas	Smart Contract, Operations, Financials
Chains	Ethereum Mainnet (Chain ID: 1)
Report Version	1.0.0
Assessment Period	2026-04-23 to 2026-05-06
Date of Publication	2026-05-08
Requested by	Non-issuer

1. Methodology

1.1 Rating Standard and Assessment Framework

This report is produced under the **Meridion Risk Rating Standard v1**. The engagement was conducted by a team combining smart contract security specialists, financial risk analysts, and formal methods engineers.

Each independent domain receives a risk rating of **Low**, **Medium**, or **High**:

- **Low** applies when no material adverse condition was identified within the assessed scope and residual risks are ordinary for the asset type.
- **Medium** applies when a material weakness, dependency, opacity, concentration, or stress scenario exists but is contingent, mitigated, not currently causing holder harm, or primarily a future-risk driver.
- **High** applies when a direct or credible path exists to material holder loss, unauthorized issuance, severe depeg, impaired transferability, asset shortfall or misrepresentation, governance or administrator capture, or operational failure.

The composite risk rating is derived from the three domain ratings using the following labels:

- **Minimal:** all three domain ratings are Low, with no material identified weakness beyond ordinary residual risk for the asset type.
- **Low:** no domain rating reaches High, and at most one reaches Medium; any Medium condition is isolated or future-oriented, with no immediate consequence for holders.
- **Moderate:** no domain rating reaches High, but multiple domains carry a Medium rating, or one Medium domain carries direct consequence, structural importance, or meaningful interaction with another domain.
- **Elevated:** at least one domain rating reaches High, but the condition remains contingent, is not actively causing holder harm, and does not currently show immediate adverse consequences.
- **High:** immediate adverse consequences are present, or an identified High domain condition bears directly on holders.

- **Severe:** multiple domains are critically compromised, or a single compromised domain produces cascading failure across the asset.

Each domain and the composite conclusion also receive a confidence rating of **Low**, **Medium**, or **High**. Confidence measures the reliability, completeness, independence, recency, and reproducibility of the evidence supporting the risk rating. Confidence does not reduce or soften the risk rating; instead, it tells the reader how strongly the rating is supported and whether material scope limitations reduce certainty.

1.2 Review Techniques Applied

SMART CONTRACTS: FUNCTIONALITY AND SECURITY

- **Runtime entry-point catalogue:** reconstruction of the complete externally callable runtime surface from deployed bytecode and verified source artifacts
- **Manual code review:** line-by-line inspection of all in-scope source files by independent security specialists
- **Edge-case and exploit-negative review:** targeted analysis of protocol-specific invariants, failure modes, access-control boundaries, replay protections, and upgrade assumptions
- **Formal verification:** direct deployed-bytecode verification of hidden calldata surface, covering selectors outside the complete runtime catalogue and malformed calldata shorter than 4 bytes
- **Fork-based behavioral testing:** live-chain execution of representative positive and negative behavioral tests against deployed bytecode using Foundry; test counts, entry-point coverage, and PASS/FAIL status are reported in the bytecode assurance section
- **AI-assisted analysis:** automated pattern detection and anomaly scanning across the full codebase to supplement human review

OPERATIONS: KEY MANAGEMENT AND ADMINISTRATIVE CONTROL

- **Role mapping:** reconstruction of deployment and administrative authority from on-chain state and historical events
- **Key management review:** assessment of HSM, MPC, and key ceremony controls based on SOC reports and public disclosures
- **Monitoring and alerting:** assessment of on-chain event alerting coverage and anomaly detection arrangements for privileged operations and administrative actions
- **Recovery assessment:** review of signer loss, compromise, and administrative recovery procedures

FINANCIALS: UNDERLYING ASSETS AND COUNTERPARTIES

- **Reserve attestation analysis:** comparison of attestation disclosures against on-chain liabilities and supply metrics
- **Counterparty profiling:** identification of issuer, custodian, banking, and attestation dependencies and their risk posture
- **Liquidity analysis:** assessment of redemption capacity and market depth across DEX and CEX venues
- **Scenario analysis:** review of economic stress scenarios and their implications for solvency, redemptions, and price stability.

2. Executive Summary

Subject Overview

USD Coin (USDC) is a fiat-collateralised payment stablecoin issued by Circle Internet Financial, LLC. Each USDC token is redeemable at par for one US dollar through Circle's institutional redemption platform (Circle Mint), with reserves held primarily in short-duration US Treasury securities and regulated bank deposits. USDC is natively issued across multiple blockchain networks; as of the assessment snapshot (block 24,941,472 on Ethereum Mainnet, 2026-04-23), the Ethereum on-chain total supply was approximately 54.43 billion USDC. Aggregate circulating supply across all chains, as attested by Deloitte and Touche LLP for the period ending April 30, 2026, was approximately 77.36 billion USDC. The residual approximately 22.93 billion USDC outstanding on non-Ethereum chains (Solana, Base, Arbitrum, Polygon, and others) was not independently verified in this investigation and relies on the Deloitte attestation for coverage.

KYC Gating

Secondary-market holding of USDC does not require KYC; any Ethereum address may hold, transfer, or receive USDC without identity verification. Minting (primary issuance) is KYC-gated: only addresses configured as authorised minters through the MinterAdmin contract may call `mint`, and access to Circle Mint (the institutional issuance channel) requires full onboarding and compliance approval. Redemption to US dollars is similarly restricted to institutional counterparties onboarded to Circle Mint with full KYC/AML verification; retail holders must exit via exchange partners or secondary markets. An on-chain blacklisting mechanism is built into the FiatTokenV2_2 implementation: the Blacklister role may freeze (`blacklist`) or unfreeze (`unBlacklist`) any Ethereum address, after which that address cannot send, receive, approve, or be approved for USDC transfers. The blacklisting mechanism is used to implement OFAC sanctions compliance and to respond to law enforcement requests. The Blacklister role is currently held by EOA `0x0a06be16275b95a7d2567fbdae118b36c7da78f9`, which operates without a publicly documented approval workflow.

Overall Risk Rating: Low

Composite Confidence: Low

USDC presents a well-established risk profile characterised by a highly capable smart contract codebase with a single Low-severity finding, 100% reserve backing attested by a Big Four accounting firm, and broadly strong regulatory standing across US and EU jurisdictions. The composite risk rating is **Low** because only the operational security domain reaches a risk score of Medium: the concentration of the highest-privilege roles (proxy admin and implementation owner) in externally owned accounts with no publicly disclosed key management arrangement creates a contingent risk that is not currently causing holder harm and has no adverse incident record. The financial domain risk is Low, reflecting fully attested reserves composed primarily of short-duration US government instruments and regulated bank deposits, with throughput constraints rather than insolvency as the primary stress-scenario risk. Composite confidence is **Low** solely because operational confidence is Low: the proxy admin and implementation owner are EOAs with immediate authority, and no public evidence confirms HSM/MPC custody, second approval, emergency workflow, monitoring thresholds, or change-control procedures for those highest-privilege roles.

Smart Contract Security Summary

SEVERITY	COUNT	RESOLVABLE
Critical	0	0
High	0	0
Medium	0	0
Low	1	1

The review did not identify any exploitable vulnerability within the assessed scope. The single finding, SEC-01, concerns the single-step ownership transfer pattern in `transferOwnership`: an input error by the owner EOA could permanently and irrecoverably transfer administrative authority to an uncontrolled address. This is gated by the `onlyOwner` modifier and requires no external attacker involvement. The contract system implements comprehensive access-control modifiers on all privileged functions, SafeMath-based arithmetic throughout, EIP-712 typed signature verification with chain-ID binding and per-address nonce tracking, and a fully locked initializer stack (version 3). The proxy upgrade mechanism is atomic: a failed initialiser call during `upgradeToAndCall` reverts the entire transaction, preventing a half-upgraded state.

Smart Contract Risk Score: Low | Confidence: High

Operational Security Summary

The primary operational risk driver is the concentration of the two highest-privilege roles in externally owned accounts with no publicly disclosed key management arrangement. The proxy admin (`0x807a96288a1a408dbc13de2b1d087d10356395d2`) can replace the entire token implementation in a single transaction with no on-chain timelock; the implementation owner (`0xfcb19e6a322b27c06842a71e8c725399f049ae3a`) can reassign all four operational roles (blacklister, pauser, masterMinter, rescuer) unilaterally. Neither HSM, MPC, hardware security key arrangement, nor a second-approval requirement is publicly documented for these roles. Circle references SOC 2 Type II certification in general disclosures, but this does not constitute a public key management disclosure for specific role addresses. No known key compromise, unauthorised minting, malicious upgrade, or operational control failure has been identified in the contract's history. The on-chain administration record shows evidence of operational discipline: three paired and reversed proxy admin changes consistent with key rotation rehearsals, and routine blacklister and pauser rotations at multi-year intervals. Risk is rated Medium because the adverse condition is contingent and no operational failure is known; confidence is Low because the controls that would prevent unilateral EOA misuse or compromise are not independently verifiable.

Opsec Risk Score: Medium | Confidence: Low

Financial Summary

USDC reserves are fully backed at 100% per the most recent Deloitte attestation (April 30, 2026), composed primarily of short-duration US Treasuries (60.7%) and overnight repo (0.7%) held in the SEC-registered Circle Reserve Fund (2a-7, BlackRock managed, BNY Mellon custodied), with 38.6% in regulated bank deposits. Reserve quality is high; the primary financial risks are bank deposit counterparty concentration (partially opaque: the $11.28 billion in "other bank deposits" is not attributed to named institutions) and the absence of

a bankruptcy-remote legal structure for USDC holders under current US law (holders have a contractual redemption right against Circle, not a direct claim on specific reserve assets). Redemption capacity under mass-exit conditions is constrained by banking-hour and settlement-throughput limits rather than reserve adequacy. Confidence is Medium because cross-chain supply (approximately $22.93 billion USDC on non-Ethereum chains) was not independently verified, redemption throughput is not publicly disclosed, and banking counterparties for the "other deposits" tranche are unnamed.

Financial Risk Score: Low | Confidence: Medium

Scope Limitations

- **Other deployment chains (Solana, Base, Arbitrum, Polygon, Optimism, Avalanche, and others):** Native USDC issuance and smart contract deployments on non-Ethereum chains were not assessed in this investigation. Cross-chain supply figures rely on the Deloitte attestation. Affects confidence in the financial and smart contract domains.
- **MinterAdmin contract internal analysis:** The MinterAdmin contract (`0xe982615d461dd5cd06575bbea87624fda4e3de17`) is the current masterMinter. Its internal entry points, key management, and operational controls were assessed at the role and structural level but not subjected to the full entry-point catalogue and formal verification analysis applied to `FiatTokenProxy` and `FiatTokenV2_2`. Affects confidence in the operational security domain.
- **Off-chain operational controls:** Key management arrangements, monitoring configuration, incident response procedures, and change management gates for Circle's internal operations were not independently assessed. The SOC 2 Type II reference provides a partial institutional baseline but does not verify contract-specific controls. Affects confidence in the operational security domain.
- **Circle Mint redemption throughput:** The maximum USD volume per hour or day that Circle's institutional redemption channel can process is not publicly disclosed. Scenario 3 estimates ($2-3 billion within 6 hours) are inferred from banking infrastructure norms. Affects confidence in the financial domain.
- **Banking counterparties for "other deposits":** Circle does not publicly disclose the names of banking institutions holding the $11.28 billion "other bank deposits" reserve tranche. Affects confidence in the financial domain.

3. Part I: Smart Contract Security Analysis

Smart Contract Security Rating: Low | Confidence: High

3.1 Scope and Execution Environment

Chain: Ethereum Mainnet

Assessment snapshot block: 24,941,472 (2026-04-23)

CONTRACT	ROLE	ADDRESS	COMPILER	V
FiatTokenProxy	Proxy	`0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48`	`v0.4.24+commit.e67f0147`	Y
FiatTokenV2_2	Implementation	`0x43506849D7C04F9138D1A2050bbF3A0c054402dd`	`v0.6.12+commit.27d51765`	Y

Both contracts are verified on Blockscout. The proxy was compiled without optimisation (Solidity 0.4.24). The implementation was compiled with aggressive optimisation (10,000,000 runs, Solidity 0.6.12, Istanbul EVM). The proxy uses the ZeppelinOS legacy transparent proxy pattern, storing the implementation and admin addresses in non-standard keccak256-preimage-derived slots rather than the EIP-1967 standard slots. This has no functional impact on the entry-point catalogue but affects tooling compatibility; see Section 4.3.

3.2 Entry Point Catalogue

This investigation involves a proxy and implementation split. The following two tables list only state-modifying, externally reachable entry points. View and pure functions are excluded from display but used in the formal verification runtime.

Proxy contract entry points:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-PR-001	`changeAdmin(address)`	`ifAdmin`	High	Transfers proxy admin authority to a new address in a single step with no pending-confirmation mechanism. The previous admin immediately loses all upgrade and admin-change capability. Compromise of the proxy admin key enables an attacker to assign upgrade authority to an arbitrary address in one transaction.
EP-PR-002	`upgradeTo(address)`	`ifAdmin`	High	Atomically replaces the implementation contract address stored in the ZeppelinOS implementation slot. Requires the new address to have deployed bytecode (isContract check). A single transaction from the proxy admin can replace all FiatToken logic with arbitrary bytecode.
EP-PR-003	`upgradeToAndCall(address,bytes)`	`ifAdmin`	High	Replaces the implementation and immediately executes an arbitrary call through the proxy fallback (targeting the new implementation). The entire transaction reverts if the initialiser call fails, preventing a half-upgraded state.
EP-PR-004	`fallback()`	Public	Medium	Routes all non-admin calls to the current implementation via

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				delegatecall, sharing the proxy's storage. Payable; ETH sent without calldata is handled by this path and delegated to the implementation. All token operations reach the implementation through this entry point.

The proxy contract includes 2 additional functions that are not state-modifying (view): `admin()` (EP-PR-005) and `implementation()` (EP-PR-006).

Implementation contract entry points:

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
EP-IM-001	`burn(uint256)`	`onlyMinters`	High	Authorised minters their own balance a total supply. Require amount > 0 and bal >= amount. No exte calls; all state chang (balance, minterAllowance, totalSupply) comple atomically before th event.
EP-IM-002	`mint(address,uint256)`	`onlyMinters`	High	Authorised minters increase recipient b and total supply with their configured allowance. Requires recipient != address and recipient not blacklisted. Allowan decremented on eac successful mint.
EP-IM-003	`receiveWithAuthorization(...) [7 args]`	Public	High	EIP-3009 payment authorisation using compact (bytes) sig Enforces to == msg.sender, preven fund redirection by a Nonce is marked us execution; validAfte validBefore window enforced.
EP-IM-004	`receiveWithAuthorization(...) [9 args]`	Public	High	EIP-3009 payment authorisation using r, s) signature. Ident logic and guards to IM-003.
EP-IM-005	`transfer(address,uint256)`	Public	High	Standard ERC-20 tr from msg.sender. G whenNotPaused, notBlacklisted(send notBlacklisted(recip recipient != address Packed balanceAndBlacklis

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				updated atomically f both parties.
EP-IM-006	`transferFrom(address,address,uint256)`	Public	High	Standard ERC-20 delegated transfer. Guards: whenNotPa notBlacklisted on all parties (spender, fro Allowance decreme via SafeMath.
EP-IM-007	`transferWithAuthorization(...) [7 args]`	Public	High	EIP-3009 transfer authorisation using compact signature. receiveWithAuthoriz to == msg.sender is required; any party relay. Funds are del to the fixed to addre the signed message front-runner cannot redirect funds.
EP-IM-008	`transferWithAuthorization(...) [9 args]`	Public	High	EIP-3009 transfer authorisation using r, s) signature. Ident logic and guards to IM-007.
EP-IM-009	`blacklist(address)`	`onlyBlacklister`	Medium	Adds an address to blacklist, immediate blocking it from all t operations. Takes e a single transaction no delay.
EP-IM-010	`configureMinter(address,uint256)`	`onlyMasterMinter`	Medium	Grants a minting allowance to an ado enabling it to call mi to that amount. In pr routed through the MinterAdmin contro worker model.
EP-IM-011	`pause()`	`onlyPauser`	Medium	Halts all token trans approvals, mints, ar burns until unpause called. Takes effect immediately in a sin

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				transaction with no chain delay.
EP-IM-012	`permit(...) [5 args]`	Public	Medium	EIP-2612 gasless approval using com signature. Sets spe allowance without a separate approve transaction. Sequen per-address nonce prevents replay.
EP-IM-013	`permit(...) [7 args]`	Public	Medium	EIP-2612 gasless approval using split s) signature. Same and guards as EP-I
EP-IM-014	`removeMinter(address)`	`onlyMasterMinter`	Medium	Revokes minting sta and zeroes the allow of a configured mint address.
EP-IM-015	`transferOwnership(address)`	`onlyOwner`	Medium	Immediately transfe implementation own to a new address in single step. No two- confirmation pattern input error permane disables all owner-g functions. See SEC
EP-IM-016	`unBlacklist(address)`	`onlyBlacklister`	Medium	Removes an addres the blacklist, restori ability to participate token operations. Ta effect immediately.
EP-IM-017	`unpause()`	`onlyPauser`	Medium	Resumes all token operations after a p Callable only by the current pauser.
EP-IM-018	`updateBlacklister(address)`	`onlyOwner`	Medium	Reassigns the black role to a new addres immediately and wit confirmation delay.
EP-IM-019	`updateMasterMinter(address)`	`onlyOwner`	Medium	Reassigns the masterMinter role to new address immed Can sever or replac

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				MinterAdmin mint governance structur single transaction.
EP-IM-020	`updatePauser(address)`	`onlyOwner`	Medium	Reassigns the paus to a new address immediately and wit confirmation delay.
EP-IM-021	`updateRescuer(address)`	`onlyOwner`	Medium	Assigns a rescuer address. Currently u (zero address).
EP-IM-022	`approve(address,uint256)`	Public	Low	ERC-20 allowance s Classic approve-the transferFrom front-r race is mitigated by availability of increaseAllowance decreaseAllowance
EP-IM-023	`cancelAuthorization(address,bytes32,bytes)`	Public	Low	Marks an EIP-3009 bytes32 nonce as u a given authoriser, preventing future submission of a sign authorisation bearin nonce. Compact sig variant.
EP-IM-024	`cancelAuthorization(...) [5 args]`	Public	Low	Split-signature varia cancelAuthorization Identical effect; calle must provide a valid signature from the authoriser.
EP-IM-025	`decreaseAllowance(address,uint256)`	Public	Low	Safely decrements a spender's allowance SafeMath, preventin underflow when red a large allowance.
EP-IM-026	`increaseAllowance(address,uint256)`	Public	Low	Safely increments a spender's allowance SafeMath. Preferred approve for adjustin existing allowances.
EP-IM-027	`initialize(...) [8 args]`	Public (frozen)	Low	V1 initialiser. Perma locked by the versio

ID	SIGNATURE	ACCESS GATED?	CRITICALITY	DESCRIPTION
				guard (_initializedVe == 3); every call rev immediately. Not ca in the current deploy
EP-IM-028	`initializeV2(string)`	Public (frozen)	Low	V2 initialiser. Perma locked by the versio guard.
EP-IM-029	`initializeV2_1(address)`	Public (frozen)	Low	V2.1 initialiser. Permanently locked version guard.
EP-IM-030	`initializeV2_2(address[],string)`	Public (frozen)	Low	V2.2 initialiser. Permanently locked version guard.
EP-IM-031	`rescueERC20(address,address,uint256)`	`onlyRescuer`	Low	Recovers ERC-20 t sent to the USDC c address. Currently inoperable because rescuer role is unse address).

The implementation contract includes 24 additional functions that are not state-modifying (view or pure): EP-IM-032 through EP-IM-055.

Overloaded functions in the table are abbreviated as `name(...) [N args]`, where `N` is the total parameter count.

3.3 Bytecode Surface Attestation

As capital held in on-chain assets grows, the Solidity compiler (`solc`) and deployment pipeline become increasingly attractive supply-chain attack targets. A compromised compiler, build process, or deployment artifact could insert hidden trap doors that are not visible in source-level review but are present in deployed bytecode. Meridion therefore separates bytecode assurance into two complementary controls: formal verification of hidden calldata surface and fork-based behavioral tests of intended entry-point behavior on deployed bytecode.

Input artifact hashes (Keccak-256 of deployed bytecode):

CONTRACT	ROLE	ADDRESS	BYTECODE HASH (KECCAK-256)
FiatTokenProxy	Proxy	`0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48`	`0xd80d4b7c890cb9d6a4893e6b52`
FiatTokenV2_2	Implementation	`0x43506849D7C04F9138D1A2050bbF3A0c054402dd`	`0xcdfb7d322961af3acae7a8f7ee`

Verification engine: The *Meridion Formal Verification Engine v1* is a custom-built symbolic execution environment executing EVM bytecode that supports JUMPI-tracing and SMT solving to verify the absence of trapdoors.

3.3.1 HIDDEN-SURFACE FORMAL VERIFICATION

The complete runtime catalogue of entrypoints (6 proxy entries, 55 implementation entries) serves as the exclusion set for hidden-surface verification. The report table in Section 3.2 is abridged for the implementation to state-modifying functions only; all 55 runtime selectors were used in the FV exclusion set.

FiatTokenProxy: Bytecode Surface Cases

Formal verification of the deployed FiatTokenProxy bytecode produced CONFIRMED results for both hidden-surface cases. The FiatTokenProxy uses the ZeppelinOS legacy transparent proxy pattern, storing the implementation address in a non-standard keccak256-preimage-derived storage slot `keccak256("org.zeppelinos.proxy.implementation")` rather than the EIP-1967 standard slot. The FV engine seeded this slot with the expected implementation address as a concrete initial storage state before symbolic execution, allowing the symbolic executor to confirm that all feasible delegatecall paths route exclusively to the fixed implementation address.

For unknown 4-byte selectors, 2 feasible paths were found: one REVERT path (non-admin call with unknown selector reverts via the admin gate) and one DELEGATECALL path routing to the fixed implementation address. 6 candidate branches were pruned as infeasible by the SMT solver. For short calldata, the same classification holds: 2 paths, one REVERT and one DELEGATECALL to the fixed implementation.

CASE	CONSTRAINT	CLASSIFICATION	VERDICT
Unknown 4-byte selectors	selector not in the complete runtime selector catalogue	delegates to fixed implementation or reverts	CONFIRMED
Short calldata	calldata_size < 4	delegates to fixed implementation or reverts	CONFIRMED

FiatTokenV2_2: Bytecode Surface Cases

Formal verification of the deployed FiatTokenV2_2 bytecode produced CONFIRMED results for both hidden-surface cases.

For short calldata (calldata_size < 4), a single path was found and it always reverts. This is confirmed: the implementation's Solidity-generated dispatcher reverts immediately when the input is too short to contain a valid 4-byte selector.

For unknown 4-byte selectors, 16 revert paths were found exhaustively and 57 candidate branches were pruned as infeasible. No non-reverting path was found. The implementation's dispatcher exhaustively rejects all calldata whose 4-byte selector is not among the 55 known selectors, confirming the absence of hidden callable surface.

CASE	CONSTRAINT	CLASSIFICATION	VERDICT
Unknown 4-byte selectors	selector not in the complete runtime selector catalogue	always reverts	CONFIRMED
Short calldata	calldata_size < 4	always reverts	CONFIRMED

Overall verdict: CONFIRMED

All four hidden-surface absence and proxy-routing cases are fully classified. No unexpected non-reverting hidden selector path was found in either contract. The proxy confirms that all delegatecall paths route exclusively to the expected implementation address `0x43506849D7C04F9138D1A2050bbF3A0c054402dd`. The implementation confirms that all unknown-selector paths revert.

3.3.2 FORK-BASED BEHAVIORAL TESTS

Fork-based behavioral tests were executed against the deployed FiatTokenProxy `0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48` and FiatTokenV2_2 implementation `0x43506849D7C04F9138D1A2050bbF3A0c054402dd` on an Ethereum mainnet Foundry fork at block 24,941,472.

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-PR-001	`changeAdmin`	PASS: proxy admin transfers admin authority to a new address	PASS: non-admin call reverts
EP-PR-002	`upgradeTo`	PASS: proxy admin upgrades to a new implementation address	PASS: non-admin call reverts
EP-PR-003	`upgradeToAndCall`	PASS: proxy admin upgrades and executes initializer data atomically	PASS: non-admin call reverts
EP-IM-001	`burn`	PASS: authorised minter burns its own balance and supply decreases accordingly	PASS: unauthorised caller reverts
EP-IM-002	`mint`	PASS: authorised minter mints to a valid recipient within allowance	PASS: unauthorised caller reverts
EP-IM-003	`receiveWithAuthorization (bytes)`	PASS: valid compact-signature payment authorization transfers funds to the intended receiver	PASS: wrong receiver call reverts
EP-IM-004	`receiveWithAuthorization (vrs)`	PASS: valid split-signature payment authorization transfers funds to the intended receiver	PASS: wrong receiver call reverts
EP-IM-005	`transfer`	PASS: succeeds for a non-blacklisted sender with sufficient balance	PASS: reverts on insufficient balance
EP-IM-006	`transferFrom`	PASS: succeeds with valid allowance and sufficient balance	PASS: reverts without allowance
EP-IM-007	`transferWithAuthorization (bytes)`	PASS: valid compact-signature authorization transfers funds to the signed recipient	PASS: expired authorization reverts
EP-IM-008	`transferWithAuthorization (vrs)`	PASS: valid split-signature authorization transfers funds to the signed recipient	PASS: expired authorization reverts
EP-IM-009	`blacklist`	PASS: blacklister freezes a target address	PASS: unauthorised caller reverts
EP-IM-010	`configureMinter`	PASS: masterMinter assigns minting allowance to a minter	PASS: unauthorised caller reverts
EP-IM-011	`pause`	PASS: pauser halts token operations	PASS: unauthorised caller reverts
EP-IM-012	`permit (bytes)`	PASS: valid EIP-2612 compact signature sets allowance	PASS: expired signature reverts

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-IM-013	`permit (vrs)`	PASS: valid EIP-2612 split signature sets allowance	PASS: expired signature reverts
EP-IM-014	`removeMinter`	PASS: masterMinter removes a configured minter	PASS: unauthorised caller reverts
EP-IM-015	`transferOwnership`	PASS: owner transfers implementation ownership to a new address	PASS: unauthorised caller reverts
EP-IM-016	`unBlacklist`	PASS: blacklister restores a frozen address	PASS: unauthorised caller reverts
EP-IM-017	`unpause`	PASS: pauser restores token operations after a pause	PASS: unauthorised caller reverts
EP-IM-018	`updateBlacklister`	PASS: owner reassigns the blacklister role	PASS: unauthorised caller reverts
EP-IM-019	`updateMasterMinter`	PASS: owner reassigns the masterMinter role	PASS: unauthorised caller reverts
EP-IM-020	`updatePauser`	PASS: owner reassigns the pauser role	PASS: unauthorised caller reverts
EP-IM-021	`updateRescuer`	PASS: owner reassigns the rescuer role	PASS: unauthorised caller reverts
EP-IM-022	`approve`	PASS: succeeds for a regular caller setting allowance	PASS: reverts while the token is paused
EP-IM-023	`cancelAuthorization (bytes)`	PASS: valid compact-signature cancellation marks an authorization nonce unusable	PASS: invalid signature reverts
EP-IM-024	`cancelAuthorization (vrs)`	PASS: valid split-signature cancellation marks an authorization nonce unusable	PASS: invalid signature reverts
EP-IM-025	`decreaseAllowance`	PASS: decreases an existing allowance safely	PASS: underflow attempt reverts
EP-IM-026	`increaseAllowance`	PASS: increases an existing allowance safely	PASS: reverts while the token is paused
EP-IM-027	`initialize`	N/A: positive path is permanently frozen on the live deployment	PASS: frozen initializer call reverts
EP-IM-028	`initializeV2`	N/A: positive path is permanently frozen on the live deployment	PASS: frozen initializer call reverts

ENTRY POINT	FUNCTION	POSITIVE TEST	NEGATIVE TEST
EP-IM-029	`initializeV2_1`	N/A: positive path is permanently frozen on the live deployment	PASS: frozen initializer call reverts
EP-IM-030	`initializeV2_2`	N/A: positive path is permanently frozen on the live deployment	PASS: frozen initializer call reverts
EP-IM-031	`rescueERC20`	PASS: rescuer recovers ERC-20 tokens sent to the proxy address	PASS: unauthorised caller reverts

The proxy fallback (`EP-PR-004`) was not counted as a separate required case because it is not a named selector. It was exercised implicitly by every implementation entry-point test, since those calls were sent through the deployed proxy and therefore traversed the fallback delegatecall path.

An optional fork smoke test for a selector outside the runtime catalogue was not run and was not counted as a required case; formal verification remains the authoritative hidden-surface control.

Fork-test overall result: PASS (64/64 required cases passed; 30 positive cases, 34 negative cases, all 34 named state-modifying entry points exercised)

3.3.3 BYTECODE ASSURANCE CONCLUSION

Formal verification and fork testing answer different questions. Formal verification provides exhaustive assurance over hidden calldata surface within its modelled constraints: unknown selectors and malformed short calldata. Fork tests provide sampled behavioral assurance that the deployed bytecode performs representative intended operations and rejects representative invalid operations.

The combined bytecode assurance evidence for this assessment is as follows. FV of the proxy is CONFIRMED for both cases: all feasible delegatecall paths route exclusively to the expected implementation address `0x43506849D7C04F9138D1A2050bbF3A0c054402dd` , and non-admin calls with unknown selectors or short calldata revert. FV of the implementation is CONFIRMED for both cases: unknown selectors always revert (16 revert paths; 57 infeasible branches pruned), and short calldata always reverts. Fork tests are PASS (64/64 required cases). The combined evidence provides complete bytecode assurance: formal verification exhaustively confirms the hidden-surface absence claims and proxy routing integrity, while fork tests confirm representative intended-operation and invalid-operation behaviour across all 34 named state-modifying entry points. This evidence supports a high-confidence bytecode-assurance claim and the smart contract confidence rating is High.

3.4 Edge-Case Analysis

Edge-case analysis was conducted independently by a human security researcher and advanced AI tooling for all Critical and High entry points using line-by-line source code review. Key findings are summarised below.

EDGE CASE	STATUS	EVIDENCE
Zero-address recipient in mint	Safe	require(_to != address(0)) enforced in FiatTokenV1.mint; reverts.
Zero-amount burn	Safe	require(_amount > 0) enforced in FiatTokenV1.burn; reverts.
Mint to blacklisted address	Safe	notBlacklisted(_to) modifier in mint reverts if recipient is blacklisted.
Transfer while paused	Safe	whenNotPaused modifier on transfer, transferFrom, mint, burn reverts all operations when paused.
Blacklisted sender attempting transfer	Safe	notBlacklisted(msg.sender) in transfer reverts immediately.
Allowance overflow via increaseAllowance	Safe	SafeMath.add reverts on overflow; no way to wrap allowance around.
Zero-value transfer	Safe	Permitted per ERC-20 standard; passes all guards with no adverse state change.
EIP-3009 authorisation with expired validBefore	Safe	require(block.timestamp < validBefore) reverts expired authorisations.
EIP-3009 authorisation replay	Safe	bytes32 nonce marked used on first execution; duplicate nonce reverts.
EIP-2612 permit replay	Safe	Sequential uint256 per-address nonces; mismatched nonce reverts.
upgradeToAndCall with reverting initialiser	Safe	require(success) wrapper reverts the entire transaction; no partial upgrade state possible.
upgradeTo with non-contract address	Safe	isContract check reverts if new implementation has no deployed bytecode.
changeAdmin to zero address	Safe	require(newAdmin != address(0)) enforced in ZeppelinOS _setAdmin.
Packed balance overflowing into blacklist flag bit	Safe	_setBalance requires balance <= (1 << 255) - 1, preventing the high bit from being overwritten.
Frozen initialiser replay	Safe	All four initialiser functions require _initializedVersion to equal a specific previous version value; current version is 3, causing all calls to revert immediately.
receiveWithAuthorization with non-recipient caller	Safe	require(to == msg.sender) reverts any caller who is not the intended recipient.
transferWithAuthorization front-run fund theft	Safe	to address is fixed in the signed message; a front-runner who submits the transaction delivers funds to the intended recipient, not themselves.
burn by blacklisted minter	Safe	A blacklisted minter can still burn their existing balance (burn does not apply notBlacklisted), but cannot receive new tokens via transfer. Residual burn risk is bounded to existing minter balance and does not affect other holders.

3.5 Common Exploit Negatives

Based on line-by-line source code review by human security researchers and LLM-based reasoning, the following exploit negatives were identified:

EXPLOIT CLASS	STATUS	EVIDENCE
Reentrancy	Mitigated	No external calls in any user-facing state-modifying path (transfer, transferFrom, mint, burn, permit, transferWithAuthorization, receiveWithAuthorization). The only external call is in rescueERC20 (IERC20.transfer), which is the terminal action with no subsequent state reads. No ERC-777 hooks or callback patterns are implemented.
Integer overflow / underflow	Mitigated	Solidity 0.6.12 with SafeMath throughout for balance and supply arithmetic. FiatTokenV2_2 introduces explicit cap check in _setBalance (balance <= (1 << 255) - 1) to protect the packed blacklist flag bit. Allowance arithmetic uses SafeMath-based increaseAllowance and decreaseAllowance.
Access control bypass	Mitigated	All privileged functions are gated by explicit role modifiers (onlyOwner, onlyMasterMinter, onlyMinters, onlyPauser, onlyBlacklister, onlyRescuer, ifAdmin). All initialiser functions are permanently locked by the version counter (_initializedVersion == 3). No modifier is absent or commented-out on any entry point.
Front-running	Mitigated	receiveWithAuthorization enforces to == msg.sender, preventing front-run fund interception. transferWithAuthorization fixes the to address in the signed message; a front-runner cannot redirect funds. increaseAllowance and decreaseAllowance are available to avoid the classic ERC-20 approve race condition.
Oracle manipulation	Not applicable	FiatTokenV2_2 is a pure mint-and-burn stablecoin with no external price oracle dependency. No AMM pool interactions, lending rate queries, or spot-price reads are present in the contract.
Signature replay	Mitigated	All signature-consuming functions use EIP-712 typed structured data. The domain separator includes the chain ID via the assembly chainid() opcode, binding signatures to Ethereum mainnet. EIP-3009 authorisation functions use per-authoriser bytes32 nonces; EIP-2612 permit uses sequential uint256 nonces per address. Used nonces cannot be reused.
Flash loan attack	Not applicable	Flash loan attacks require price manipulation or liquidity pool manipulation, neither of which is applicable to a permissioned mint-and-burn stablecoin. Supply is controlled exclusively by authorised minters.
Denial of service	Mitigated	initializeV2_2 contained an unbounded loop over a caller-supplied array, but this function is permanently frozen (_initializedVersion == 3). All currently callable state-mutating functions operate on O(1) storage reads and writes with no unbounded loops over user-controlled input.
Upgrade proxy risk	Mitigated	The V2_2 migration (initializeV2_2) successfully migrated account state to the packed balanceAndBlacklistStates layout and is permanently locked. Prior initialiser versions are permanently disabled. Upgrade governance is analysed in Section 4.3.
Dependency and supply chain risk	Mitigated	The proxy is compiled from zos-lib v2.x (widely audited, immutably deployed). The implementation uses Circle's in-house code with inline EIP-712, EIP-2612, and EIP-3009 implementations. No live external library calls or dynamic

EXPLOIT CLASS	STATUS	EVIDENCE
		dependency resolution exists in the deployed bytecode. Compiler versions are pinned.

3.6 Security Findings Register

SEC-01: SINGLE-STEP OWNERSHIP TRANSFER WITH NO PENDING-OWNER CONFIRMATION

FIELD	DETAIL
Finding ID	SEC-01
Title	Single-step ownership transfer with no pending-owner confirmation
Severity	Low
Entry Point(s)	EP-IM-015 (`transferOwnership(address)`)
Description	`transferOwnership(address)` immediately replaces the current owner with the new address in a single transaction. There is no intermediate pending state requiring the new owner to call an accept function before the transfer finalises. This pattern is inherited from the Ownable base contract. If the caller mistypes or provides an incorrect address, ownership is permanently and irrecoverably transferred to an uncontrolled address, disabling all onlyOwner-gated functions: `transferOwnership` , `updateBlacklister` , `updateMasterMinter` , `updatePauser` , and `updateRescuer` .
Impact	If the owner EOA makes an input error, all owner-gated administrative functions become permanently inaccessible with no on-chain recovery path (unless the proxy admin upgrades to a new implementation with a reset owner). Under normal operation with a careful owner, this risk does not materialise. No external attacker can trigger this vulnerability without first compromising the owner key.
Recommendation	Adopt OpenZeppelin Ownable2Step or an equivalent two-step pattern that requires the proposed new owner to call `acceptOwnership()` before the transfer finalises. This ensures the new address is live and accessible before control is relinquished.

4. Part II: Operational Security

Operational Security Rating: Medium | Confidence: Low

4.1 Privileged Roles

Role holders at assessment snapshot:

ROLE	ADDRESS	TYPE
Proxy Admin	`0x807a96288a1a408dbc13de2b1d087d10356395d2`	EOA
Implementation Owner	`0xfcb19e6a322b27c06842a71e8c725399f049ae3a`	EOA
MasterMinter (contract)	`0xe982615d461dd5cd06575bbea87624fda4e3de17`	Contract (MinterAdmin)
MinterAdmin Owner	`0xc1d9fe41d19dd52cb3ae5d1d3b0030b5d498c704`	EOA
Blacklister	`0x0a06be16275b95a7d2567fbdae118b36c7da78f9`	EOA
Pauser	`0x4914f61d25e5c567143774b76edbf4d5109a8566`	EOA
Rescuer	`0x0000000000000000000000000000000000000000`	Unset (zero address)

Proxy Admin (`0x807a96288a1a408dbc13de2b1d087d10356395d2`): This is the highest-privilege role in the system. A single transaction from this key can replace the entire FiatTokenV2_2 implementation with arbitrary bytecode via `upgradeTo` or `upgradeToAndCall`. The proxy admin can also transfer the admin role itself via `changeAdmin`. The holder is an EOA confirmed not to be a Gnosis Safe (verified via Blockscout and Safe API). No HSM, MPC, hardware security key, or second-approval requirement is publicly documented for this role. The address has been stable since September 2018 (block 6278324), with three transient rehearsal-pattern changes (blocks 10743406, 12317806, 18963710) each reversed within 72-91 seconds. No public disclosure of a key management policy exists.

Implementation Owner (`0xfcb19e6a322b27c06842a71e8c725399f049ae3a`): Controls four role-reassignment functions (`updateBlacklister`, `updateMasterMinter`, `updatePauser`, `updateRescuer`) and `transferOwnership`. A single transaction from this key can reassign any operational role to an attacker-controlled address. The holder is an EOA confirmed not to be a Gnosis Safe. Unchanged since deployment (block 6282629, September 2018). No key management disclosure exists.

MasterMinter: MinterAdmin Contract (`0xe982615d461dd5cd06575bbea87624fda4e3de17`): The masterMinter role is held by a verified contract, not a direct EOA. The MinterAdmin implements an owner-controller-worker model: the MinterAdmin owner (`0xc1d9fe41d19dd52cb3ae5d1d3b0030b5d498c704`, an EOA) configures controllers; each controller manages one worker minter; workers call `configureMinter` on FiatToken through MinterAdmin. This structure adds meaningful separation: the MinterAdmin owner cannot mint directly. However, if the MinterAdmin owner key is compromised, an attacker can reconfigure the controller-worker assignments and ultimately redirect the entire mint pathway. The implementation owner can mitigate this by calling `updateMasterMinter` to replace the compromised MinterAdmin contract.

Blacklister (`0x0a06be16275b95a7d2567fbdae118b36c7da78f9`): Can freeze or unfreeze any Ethereum address in a single transaction (`blacklist`, `unBlacklist`). This is a compliance-critical, operationally active role: the key must remain accessible for ongoing sanctions enforcement, meaning it is likely a hot or warm key. No HSM or MPC disclosure exists. The role has been rotated three times since 2019, suggesting active key management practices. The owner can reassign via `updateBlacklister`.

Pauser (`0x4914f61d25e5c567143774b76edbf4d5109a8566`): Can halt all token operations in a single transaction (`pause`) or restore them (`unpause`). Single-key control is a deliberate design choice enabling fast incident response; requiring multi-party approval would slow emergency interventions. No key management disclosure exists. Last assigned at block 17965526 (August 2023). The owner can reassign via `updatePauser`.

Rescuer (unset, zero address): The rescuer role would allow recovery of ERC-20 tokens accidentally sent to the USDC proxy address via `rescueERC20`. Because the role holder is the zero address, `rescueERC20` is permanently inoperable in the current state: no caller can satisfy the `onlyRescuer` modifier. Any ERC-20 tokens sent to `0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48` are irrecoverable until the owner calls `updateRescuer`. This has no impact on normal token operations or supply.

Key management transparency: No HSM, MPC, hardware security key, or equivalent arrangement has been publicly disclosed for any of the EOA role holders (proxy admin, implementation owner, MinterAdmin owner, blacklister, pauser). Circle references SOC 2 Type II certification in general disclosures, but this does not constitute a public disclosure of key management arrangements for specific on-chain role addresses. The transparency gap is documented. It does not establish that key management controls are absent; it establishes that they cannot be independently verified. Because the highest-privilege roles are EOAs with immediate upgrade and role-reassignment authority, this evidence gap lowers Operational Security confidence to Low.

4.2 Administration History

The following is a chronological reconstruction of material administrative events derived from on-chain event data.

2018-08-03: AdminChanged event at block 6082473. Proxy admin set from the initial deployer address to `0x69005ff7...` during initial deployment setup.

2018-09-05: AdminChanged at block 6278324. Proxy admin changed to `0x807a9628...`, the stable admin address held to the assessment date.

2018-09-06: Batch of initial role-configuration events. PauserChanged (block 6282401) sets first pauser. MasterMinterChanged (block 6282558) sets initial master minter as an EOA. OwnershipTransferred (block 6282629) from deployer to `0xfcb19e6a...`, the current implementation owner, unchanged to the assessment date.

2018-09-06: MinterRemoved at block 6283968, removing a deployment-time test minter.

2019-01-28: MinterRemoved at block 7140662.

2019-06-12: MasterMinterChanged at block 7944634. The initial EOA masterMinter is replaced by the MinterAdmin contract (`0xe982615d...`). This is a meaningful operational improvement: direct EOA minting is replaced by the owner-controller-worker contract governance model.

2019-06-27: PauserChanged and BlacklisterChanged at blocks 8041875 and 8041867.

2020-08-27: Paired AdminChanged events at blocks 10743406 and 10743414 (within 79 seconds). Proxy admin transiently changed to `0xed24bd79...` and immediately returned to `0x807a9628...`. Pattern is consistent with a key rotation rehearsal or administrative access verification.

2021-04-06: Two MinterRemoved events at blocks 12187552 and 12187586.

2021-04-26: Paired AdminChanged events at blocks 12317806 and 12317814 (within 91 seconds). Same transient-change-and-return pattern, this time via `0xd13689e8...`. Second rehearsal event.

2023-03-10 to 2023-03-13 (SVB depeg): USDC temporarily depegged from USD following Circle's disclosure that approximately $3.3 billion of USDC reserves were held at Silicon Valley Bank (SVB) at the time of its FDIC receivership. USDC traded as low as approximately $0.87 before recovering to $1.00 after the FDIC guaranteed SVB deposits. No privileged contract functions were invoked, no emergency pause was triggered, and no key compromise or unauthorised minting occurred. This was a reserve and financial event, not an operational security event; see Section 5.

2023-08-21: PauserChanged at block 17965526 and BlacklisterChanged at block 17965524. Two role changes within two blocks, consistent with a coordinated role handover. Pauser assigned to `0x4914f61d...` (current holder); blacklister assigned to `0x10df6b6f...`.

2024-01-08: Paired AdminChanged events at blocks 18963710 and 18963716 (within 72 seconds). Third rehearsal-pattern event, transient change to `0x9999fa87...` and return to `0x807a9628...`.

2025-03-18: MinterRemoved at block 22075183.

2025-05-06: MinterRemoved at block 22427208.

2025-05-29: MinterRemoved at block 22590579.

2025-06-30: BlacklisterChanged at block 22818122. Blacklister rotated to `0x0a06be16...`, the current holder. Most recent role change at assessment date.

Pattern assessment: The administration history reflects routine operational hygiene: role rotations at multi-year intervals, three proxy admin rotation rehearsals with a consistent return-to-stable pattern, and minter lifecycle management through the MinterAdmin contract. No emergency pause events, unexpected role transfers, unauthorised admin changes, or anomalous minting events appear in the on-chain record. No operational incidents beyond the March 2023 SVB-related reserve event have been identified.

4.3 Upgrade Risk Analysis

Proxy standard: FiatTokenProxy uses the ZeppelinOS (zos-lib v2.x) legacy transparent proxy pattern. The implementation and admin addresses are stored in non-standard storage slots derived from `keccak256("org.zeppelinos.proxy.implementation")` and `keccak256("org.zeppelinos.proxy.admin")` respectively. These are not EIP-1967 standard slots. Blockscout labels this proxy as `eip1967_oz`, which is technically inaccurate: any tool that reads the EIP-1967 slots (0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc and 0xb53127684a568b3173ae13b9f8a6016e243e63b6e8ee1178d6a717850b5d6103) will read zero values rather than the actual implementation and admin addresses.

What upgrade capability grants: The proxy admin can call `upgradeTo(newImplementation)` to atomically replace the implementation address in the ZeppelinOS slot. `upgradeToAndCall(newImplementation, data)` additionally executes an arbitrary call through the proxy fallback immediately after setting the new implementation. The effect is total: a new implementation can redefine all token logic, storage interpretation, balances, supply, minting, blacklisting, and ownership structure in a single transaction.

Atomicity and initialisation: Upgrades via `upgradeToAndCall` are atomic. The new implementation is set first, then the initialiser call is made. If the initialiser reverts, `require(success)` causes the entire transaction to revert; no half-upgraded state is possible. The current version counter is `_initializedVersion == 3`, set by `initializeV2_2`. A future upgrade to a new version would require a new initialiser guarded by a version check of 4 or higher.

Storage layout compatibility: Storage layout compatibility is not enforced on-chain. FiatTokenV2_2 introduced a packed `balanceAndBlacklistStates` mapping that merges balance and blacklist state into a single `uint256` per address. Any future upgrade must preserve this layout exactly; a mismatch would silently corrupt balances or blacklist states. This risk is managed by process only: correct layout is the responsibility of Circle's engineering and audit workflow.

No on-chain timelock: No timelock is implemented at the proxy level. Once the proxy admin submits an `upgradeTo` transaction, the upgrade takes effect in the same block. Token holders have no advance notice window on-chain. The absence of a timelock enables faster incident response: a critical vulnerability could be patched in a single block. The tradeoff is that holders have no exit window before a non-emergency upgrade takes effect.

Tooling and monitoring consideration: Because FiatTokenProxy uses ZeppelinOS legacy slots rather than EIP-1967, upgrade management tooling that defaults to EIP-1967 slot reads (Hardhat upgrades plugin, OpenZeppelin Defender, Tenderly upgrade tracking) must be explicitly configured with the ZeppelinOS preimage scheme. Tools that read EIP-1967 slots will silently show null values for admin and implementation, which could lead to incorrect operational decisions.

4.4 Recovery Scenarios

SCENARIO 1: PROXY ADMIN KEY LOST OR PERMANENTLY INACCESSIBLE

FIELD	DETAIL
Detection Method	Discovered when Circle attempts to sign a proxy admin transaction (e.g., during a key access test, key rotation rehearsal, or when an upgrade is required) and finds the key inaccessible. No on-chain signal.
Recovery Possible?	No
Recovery Authority	None. The proxy admin key is the sole upgrade authority; no alternative recovery path exists on-chain.
Recovery Path	No on-chain recovery path exists. The current implementation continues to operate normally, but the proxy admin role can never be reassigned and the implementation can never be upgraded. If a critical bug is discovered in FiatTokenV2_2, there is no on-chain remedy. Off-chain options are limited to deploying a new token contract and coordinating migration of liquidity and integrations.
Prerequisites / Dependencies	Proxy admin key accessible (prerequisite that has failed in this scenario).
Operational Impact	Upgrade capability permanently frozen. All current token operations (transfers, mints, burns, blacklisting) continue unaffected. The impact is zero in the near term and potentially severe if a critical vulnerability is subsequently discovered.
Residual Risk	Permanent inability to patch the contract. A critical vulnerability in FiatTokenV2_2 would have no on-chain remedy.

SCENARIO 2: PROXY ADMIN KEY COMPROMISED

FIELD	DETAIL
Detection Method	On-chain monitoring of Upgraded and AdminChanged events on the proxy contract. Detection requires timely monitoring; the upgrade takes effect in a single block with no on-chain delay.
Recovery Possible?	Partial
Recovery Authority	Implementation owner can continue operating and rotate other roles if the malicious upgrade has not yet been applied. No on-chain remedy once a malicious upgrade is finalised.
Recovery Path	If detected before a malicious upgrade executes: implementation owner can limit blast radius by reassigning operational roles. If a malicious upgrade has been applied: no on-chain reversal is possible through the existing contract. Recovery would require off-chain coordination with exchanges, bridges, and DeFi protocols, a new token contract deployment, and migration of liquidity.
Prerequisites / Dependencies	Sub-block on-chain monitoring of proxy events; emergency response procedure activated; implementation owner key accessible.
Operational Impact	Potentially catastrophic if a malicious implementation is deployed before detection. All FiatToken logic, balances, and supply can be redefined by the attacker in a single transaction.
Residual Risk	If a malicious upgrade completes before detection and response, all USDC holders face arbitrary balance manipulation. Recovery requires off-chain coordination and a new deployment.

SCENARIO 3: IMPLEMENTATION OWNER KEY COMPROMISED

FIELD	DETAIL
Detection Method	On-chain monitoring of OwnershipTransferred, BlacklisterChanged, PauserChanged, and MasterMinterChanged events. Role changes take effect immediately in the same transaction.
Recovery Possible?	Partial
Recovery Authority	Implementation owner (if still accessible via a parallel key path before the attacker acts) or proxy admin (can upgrade to a new implementation that resets the owner).
Recovery Path	If the attacker has not yet transferred ownership: the legitimate owner (via an available backup credential) reassigns roles. If ownership has been transferred to an attacker address: the proxy admin can upgrade to a new implementation that resets the owner via a new initialiser function. This requires a prepared emergency upgrade and an intact proxy admin key.
Prerequisites / Dependencies	On-chain monitoring for role change events; proxy admin key accessible; emergency upgrade implementation prepared and audited.
Operational Impact	Attacker can mass-unblacklist sanctioned addresses, redirect the masterMinter to allow unlimited minting, or disable the pauser. Impact grows with each role reassigned before detection.
Residual Risk	If both owner and proxy admin keys are simultaneously compromised, no on-chain recovery path exists.

SCENARIO 4: ACCIDENTAL PROTOCOL PAUSE

FIELD	DETAIL
Detection Method	Immediate: all USDC transfers, approvals, mints, and burns revert. DeFi protocols integrated with USDC surface errors. On-chain monitoring of the Pause event.
Recovery Possible?	Yes
Recovery Authority	Pauser (can call unpause) or implementation owner (can reassign pauser via updatePauser to a new address).
Recovery Path	Pauser calls `unpause()` if the pauser key is accessible. If the pauser key is inaccessible, the implementation owner calls `updatePauser` to assign a new pauser address, which then calls `unpause()`.
Prerequisites / Dependencies	Pauser key accessible, or implementation owner key accessible.
Operational Impact	All USDC operations halted for the duration of the pause. DeFi protocols, exchanges, and bridges dependent on USDC transfers experience disruption. Duration depends on response time.
Residual Risk	If both pauser and owner keys are simultaneously inaccessible, the pause cannot be lifted without a proxy admin upgrade.

SCENARIO 5: FAILED OR STORAGE-CORRUPTING IMPLEMENTATION UPGRADE

FIELD	DETAIL
Detection Method	Post-upgrade testing, on-chain anomaly detection (unexpected transfer failures, corrupted balances, incorrect balanceOf return values), or user reports. No automatic on-chain rollback mechanism.
Recovery Possible?	Partial
Recovery Authority	Proxy admin (can upgrade to a corrected implementation if key is intact).
Recovery Path	Proxy admin deploys a corrected implementation that repairs the storage layout or logic error and calls upgradeToAndCall with a migration function. Storage corruption affecting the packed balanceAndBlacklistStates mapping may be irrecoverable if affected slots cannot be deterministically reconstructed from off-chain records.
Prerequisites / Dependencies	Proxy admin key accessible; corrected implementation prepared and audited; storage migration plan available if balances are corrupted.
Operational Impact	Token operations may be disrupted or produce incorrect results from the moment of upgrade until a corrective upgrade is applied. Duration depends on detection and response time.
Residual Risk	Irreversible balance corruption if a storage layout collision silently corrupts the packed balanceAndBlacklistStates mapping before detection.

SCENARIO 6: MINTERADMIN OWNER KEY COMPROMISED

FIELD	DETAIL
Detection Method	On-chain monitoring of ControllerConfigured and MinterConfigured events on the MinterAdmin (`0xe982615d...`) and FiatToken contracts.
Recovery Possible?	Yes
Recovery Authority	Implementation owner (can call updateMasterMinter to replace the MinterAdmin contract); MinterAdmin owner (can call removeController if a legitimate backup credential is available).
Recovery Path	Implementation owner calls `updateMasterMinter` pointing to a new or re-deployed MinterAdmin contract, severing the compromised mint pathway. Attacker-added minters can be removed from FiatToken by the new masterMinter via `removeMinter` .
Prerequisites / Dependencies	Implementation owner key accessible; new MinterAdmin contract prepared; on-chain monitoring for ControllerConfigured events on MinterAdmin.
Operational Impact	Attacker may authorise unlimited minting via compromised worker addresses until the masterMinter is replaced. Scale depends on detection speed.
Residual Risk	Tokens minted by attacker-controlled minters before mitigation increase total supply without reserve backing. Financial impact is addressed in Section 5.

Recovery design assessment: Recovery capability is centralised around two EOA keys: the proxy admin and the implementation owner. These two addresses are single points of failure in complementary roles: the proxy admin is the only path to upgrade-based recovery, and the implementation owner is the only path to role-reassignment-based recovery. If both keys are simultaneously compromised or inaccessible, the protocol has no on-chain recovery path. The three paired proxy admin rehearsal events in the administration history suggest Circle has tested administrative key access procedures on-chain, but no public documentation of a formal recovery runbook exists.

4.5 Multisig Security Analysis

This section is not applicable. No privileged role is held by a multisig wallet. All EOA role holders (proxy admin, implementation owner, MinterAdmin owner, blacklister, pauser) are externally owned accounts confirmed not to be Gnosis Safe contracts (verified via Blockscout and the Safe API). The MasterMinter role is held by the MinterAdmin contract, which provides structural separation for mint authorisation within its owner-controller-worker model but is itself not a multisig and is owned by an EOA. The implications of EOA role holders and the absence of on-chain multi-party approval are addressed in Sections 4.1 and 4.4.

5. Part III: Financial Analysis

Financial Risk Rating: Low | Confidence: Medium

5.1 Underlying Asset Attestation

Circle publishes monthly reserve attestation reports on its public transparency page. Attestations are conducted by **Deloitte and Touche LLP**, a Big Four accounting firm, under attestation standards issued by the American Institute of Certified Public Accountants (AICPA). Reports are published approximately 2-4 weeks after the end of each calendar month. The Circle Reserve Fund (USDXX), the primary reserve vehicle holding the Treasury and repo tranche, additionally publishes daily independent third-party portfolio reporting via BlackRock, providing intra-month visibility into the largest reserve component.

Attestation programme: Deloitte and Touche LLP, monthly

Most recent attestation report: April 30, 2026

METRIC	VALUE	SOURCE
Attested reserve balance	$77.36B	Deloitte and Touche LLP / April 30, 2026
Attested liabilities / tokens outstanding	$77.36B	Deloitte and Touche LLP / April 30, 2026
Implied collateralisation ratio	100.0%	Derived
On-chain token supply (Ethereum, snapshot block 24,941,472)	54.43B USDC	Verified via eth_call
Multi-chain aggregate supply (CoinGecko, 2026-05-05)	77.78B USDC	CoinGecko
Market price	$0.9999	CoinGecko / 2026-05-05
30-day average daily volume (CEX)	$16.40B	CoinGecko
Conservative executable DEX liquidity (swap pools only)	$803M	DeFiLlama / 2026-05-05

Reserve composition (April 30, 2026):

COMPONENT	AMOUNT (USD)	SHARE
Short-duration US Treasuries (< 3-month)	$47.00B	60.7%
Deposits at Systemically Important Financial Institutions (SIFIs)	$18.56B	24.0%
Other bank deposits	$11.28B	14.6%
Overnight reverse Treasury repo	$520M	0.7%
Total	**$77.36B**	**100%**

Supply reconciliation: The Ethereum on-chain supply (54.43 billion USDC) is approximately $22.93 billion lower than the attested aggregate circulating supply (77.36 billion USDC). This gap is consistent with USDC's extensive multi-chain deployment. USDC is natively issued by Circle on Solana, Base, Arbitrum, Polygon, Avalanche, Optimism, and other networks. The gap represents USDC outstanding on non-Ethereum chains.

Cross-chain supply was not independently verified in this investigation (status: manual or external verification required). The Deloitte attestation covers aggregate circulating supply across all chains and is treated as the authoritative total-supply figure. The approximately $0.44 billion difference between the attested supply at April 30, 2026 and the CoinGecko-reported supply at May 5, 2026 is consistent with normal issuance activity over the 5-day intervening period.

Reserve adequacy: Reserves are fully backed at 100% per attestation. Reserve assets are concentrated in short-duration, high-quality liquid assets (HQLA): US Treasuries and overnight repo account for approximately 61.4% of reserves, providing high liquidity and negligible credit risk. The bank deposit component (38.6%) introduces counterparty concentration risk at individual institutions, partially mitigated by SIFI designation of the primary deposit counterparties and post-2023 diversification following the SVB event. Reserve adequacy is assessed as sufficient.

5.2 Counterparty Risk Profile

PARTY	ROLE	JURISDICTION	RISK SUMMARY
Circle Internet Financial, LLC	Issuer	Delaware, USA	Well-capitalised, regulated stablecoin issuer; no material adverse credit events; contractual redemption structure (not direct claim on reserves).
BlackRock Advisors, LLC	Reserve Fund Manager (Circle Reserve Fund)	USA	World's largest asset manager; negligible operational and reputational risk for USDC; USDXX assets legally segregated and BNY Mellon custodied.
The Bank of New York Mellon	Custodian (Circle Reserve Fund)	Delaware, USA	US G-SIB and SIFI; enhanced regulatory supervision; primary custodian for the $47.5 billion Treasury and repo tranche.
Unnamed banking counterparties	Other deposits	USA (partial)	$11.28 billion in deposits at institutions not publicly named; SVB-type concentration risk cannot be fully ruled out.
Deloitte and Touche LLP	Attestor	USA	Big Four accounting firm; AICPA attestation standards; monthly point-in-time reserve confirmation; not a continuous audit.

Circle Internet Financial, LLC: Circle is the sole issuer of USDC since the dissolution of the Centre Consortium in 2023. Circle is a Delaware-incorporated, privately held fintech company with significant institutional backing, holding money transmitter licences across all 50 US states and DC, a FinCEN MSB registration, a NYDFS BitLicence, and an Electronic Money Institution (EMI) licence from the ACPR (France) enabling MiCA-compliant issuance across the EEA. No material adverse credit events are known as of the assessment date. USDC holders have a contractual redemption right against Circle at 1:1 USD, subject to onboarding and AML/KYC compliance. Reserves are held in segregated accounts and the Circle Reserve Fund, but the legal structure does not create a trust or direct beneficial ownership arrangement for USDC holders under current US law. If Circle were to enter insolvency, holders would be unsecured creditors or potentially beneficiaries depending on the applicable state law and insolvency proceeding. Pending US

federal stablecoin legislation would, if enacted in current proposed form, mandate stronger bankruptcy-remote structures. The March 2023 SVB incident (approximately $3.3 billion in USDC reserves at SVB at the time of FDIC receivership) caused a temporary depeg; Circle confirmed full recovery after FDIC depositor guarantee. Post-2023, Circle disclosed increased diversification of banking counterparties.

BlackRock Advisors, LLC: Manager of the Circle Reserve Fund (ticker: USDXX), an SEC-registered 2a-7 government money market fund. BlackRock is the world's largest asset manager by AUM; reputational and operational risk is low. USDXX assets are legally segregated from BlackRock's corporate estate; fund investors (Circle on behalf of USDC holders) hold beneficial interests in the fund's portfolio. No known adverse regulatory actions relevant to USDC reserve management.

The Bank of New York Mellon Corporation: BNY Mellon is the custodian for the Circle Reserve Fund and USDC reserves held in US government securities. It is a US SIFI and globally systemically important bank (G-SIB), subject to enhanced regulatory supervision including Federal Reserve stress testing. As a G-SIB, BNY Mellon benefits from an implicit public backstop; credit risk for custody purposes is low. Various regulatory engagements typical of a G-SIB institution have occurred over the years; none are known to be directly relevant to USDC custody.

Unnamed banking counterparties: The $11.28 billion in "other bank deposits" and $18.56 billion in "SIFI deposits" are held at institutions not all publicly named by Circle. The SIFI designation of the primary deposit bank(s) partially mitigates concentration risk, but the concentration at unnamed "other" banks cannot be independently assessed. A repetition of the SVB scenario at a named "other bank deposits" counterparty represents a residual risk that cannot be quantified without counterparty disclosure.

Deloitte and Touche LLP: The attestation programme provides monthly point-in-time confirmation that reserve assets meet or exceed circulating liabilities. Attestation under AICPA standards provides meaningful but bounded assurance: it is not a continuous audit, does not verify individual asset title beyond the attestation point, and does not provide assurance over operational controls between attestation dates. Deloitte is a Big Four firm with low reputational and operational risk.

5.3 Liquidity Risks and Scenario Analysis

5.3.1 LIQUIDITY PROFILE

Issuer redemption: USDC redemption to US dollars is processed exclusively through Circle Mint, accessible to institutional counterparties only. Individual holders must exit via exchange partners or secondary markets. Institutional direct redemption operates at T+0 or T+1 during US banking hours, with settlement depending on USD wire infrastructure. KYC/AML onboarding is required. No contractual redemption gate is disclosed, but settlement infrastructure creates practical throughput limits not publicly quantified by Circle. Weekend and bank holiday delays are possible.

On-chain liquidity: Conservative executable DEX liquidity (swap pools only, excluding lending and restricted pools) is approximately $803.6 million. Reported DEX TVL across all pool types is approximately $8.19 billion, but the majority of this (approximately $7.38 billion) is illiquid for exit purposes: USDC deposited in lending protocols (Maple Finance approximately $3.07 billion, Morpho approximately $1.3 billion, Spark approximately $946 million) cannot be immediately withdrawn by a third party seeking to reduce USDC exposure.

Exchange liquidity: Binance reports approximately $2.27 billion per day in USDC volume; Kraken approximately $98.5 million per day; Coinbase Exchange approximately $33.5 million per day. These are reported turnover figures, not confirmed order-book depth. In stressed conditions, CEX bid-side depth can compress materially.

VENUE	TYPE	TVL / DEPTH	NOTES
Swap pools (aggregate, Ethereum)	DEX	$803.6M	Conservative executable; lending/ restricted excluded
Lending protocols (Maple, Morpho, Spark, others)	DeFi lending	$7.38B	Not immediately executable as swap exit
Binance	CEX	$2.27B/day volume	Turnover, not confirmed depth
Kraken	CEX	$98.5M/day volume	Turnover, not confirmed depth
Coinbase Exchange	CEX	$33.5M/day volume	Turnover, not confirmed depth

The $803.6 million in conservative DEX liquidity is the reliable lower bound for on-chain exit capacity in a stressed scenario. Stress scenarios involving multi-billion USD exits within short windows would exceed on-chain DEX capacity and push demand to the Circle direct-redemption channel, which is constrained by banking-hour settlement throughput.

5.3.2 SCENARIO ANALYSIS

Starting reserve position (Ethereum on-chain USDC outstanding, USD): $54,419,270,369. This is the USD value of the 54,429,775,315.94 USDC Ethereum on-chain token supply at the snapshot market price, not a separate token-quantity figure. **Full attested reserve position (all chains, April 30, 2026):** ~$77,360,000,000

Scenario 1: Base Case

FIELD	DETAIL
Trigger Conditions	Normal operating environment; redemption demand within historical norms; collateral fully attested at 100%.
Effect on Collateral	Reserves are 100% backed with a reserve composition dominated by HQLA (short-duration Treasuries, overnight repo). No impairment expected under base conditions.
Liquidity Runway	Estimated approximately $500 million in net daily redemptions. This is comfortably serviced by Circle Mint institutional throughput and secondary market liquidity combined.
Anticipated Investor Actions	Routine portfolio management; no elevated redemption pressure; secondary market trades near $1.00 parity.
Conclusion	No risk to solvency or peg stability under base conditions. USDC operates as designed.
Impact	Low

Scenario 2: Market Stress (Rate Shock)

FIELD	DETAIL
Trigger Conditions	A 200bps rise in short-duration US Treasury yields (emergency Federal Reserve action or equivalent macro shock) causes mark-to-market losses on the $47 billion Treasury tranche. Concurrent elevated redemption demand.
Effect on Collateral	At a maximum 90-day duration, a 200bps shock produces an estimated mark-to-market loss of approximately $231 million (approximately 0.3% of total reserves). This is a temporary unrealised loss; Treasuries held to maturity recover par. The Circle Reserve Fund (2a-7) is required to maintain stable NAV; break-the-buck risk is extremely low given sub-3-month maturities and SEC-regulated structure. The bank deposit tranche ($29.84 billion) creates a secondary concern if rate stress triggers bank instability analogous to SVB-2023.
Liquidity Runway	Modelled at $5 billion in net redemptions over 24 hours. Remaining reserves: approximately $72.1 billion versus approximately $72.1 billion remaining liabilities. The T-bill maturity ladder enables rapid reserve liquidity recovery within days.
Anticipated Investor Actions	Elevated redemption demand from institutional holders and DeFi protocol de-risking; secondary market discount of approximately 0.3% to 1.0% during acute stress.
Conclusion	Solvent and operational. Reserves remain fully adequate even at $5 billion daily redemption pace. The critical risk is not insolvency but the potential for a bank instability event among the deposit counterparties if rate stress is sustained and severe.
Impact	Medium

Scenario 3: Bank Run (25% of circulating supply redeemed within 6 hours)

FIELD	DETAIL
Trigger Conditions	A severe confidence shock triggers coordinated, rapid redemption of approximately $19.34 billion (25% of total circulating supply of $77.36 billion) within a 6-hour window.
Effect on Collateral	Total reserves are fully sufficient ($77.36 billion backing $77.36 billion). The constraint is settlement throughput, not reserve adequacy. Circle Mint institutional redemptions are estimated at $2-3 billion within a 6-hour window, constrained by USD wire settlement infrastructure. Conservative DEX liquidity provides approximately $803.6 million in immediate on-chain capacity.
Liquidity Runway	Total executable within 6 hours: approximately $3-4 billion. Unmet demand: approximately $15-16 billion (queued, not defaulted). Reserves remain fully intact; the unmet demand is a settlement timing constraint.
Anticipated Investor Actions	Secondary market USDC discounts of approximately 2% to 8% as DEX pool depth is exhausted; panic-driven demand compounds. Institutional holders seek direct redemption; retail holders face exchange-level liquidity constraints.
Conclusion	Solvent but gated. Total reserves are sufficient to honour all redemptions if processed over multiple days. The critical risk is not insolvency but a sustained peg break and loss of market confidence during the redemption queue clearance period. Circle would likely implement redemption queuing and communicate timeline to holders.
Impact	High

Scenario 4: Oracle Failure / Price Feed Manipulation

FIELD	DETAIL
Trigger Conditions	The primary Chainlink USDC/USD price oracle on Ethereum returns an anomalous value ($0.95) or becomes stale for 15 minutes, triggering automated liquidation logic in DeFi protocols that use USDC as collateral or a quote asset.
Effect on Collateral	Circle's direct-redemption mechanism does not use an external oracle; issuer operations are unaffected. DeFi impact: USDC deposited in protocols using USDC oracle feeds (Aave v3, Compound v3, and others) may be misvalued, causing unwanted liquidations or protocol freezes. Total DeFi lending TVL at potential risk: approximately $500 million.
Liquidity Runway	Estimated $500 million in DeFi-triggered and panic-driven redemptions. Remaining reserves: approximately $76.86 billion. Oracle failure does not create issuer insolvency risk; DeFi protocols may pause or liquidate independently.
Anticipated Investor Actions	DeFi protocol users face automated liquidations or frozen positions; secondary market secondary price feeds (DeFiLlama at $0.9999) provide reassurance within minutes. Self-corrects once oracle is restored or backup feeds take effect.
Conclusion	Solvent and operational at the issuer level. DeFi protocols may experience temporary operational disruption. The scenario is limited in scale and duration given backup oracle mechanisms and secondary price confirmation.
Impact	Medium

Scenario 5: Custodian Failure (BNY Mellon 48-hour outage)

FIELD	DETAIL
Trigger Conditions	BNY Mellon, the primary custodian for the Circle Reserve Fund, is unable to process withdrawals or settle transactions for 48 hours due to an operational incident, cyber attack, or regulatory freeze.
Effect on Collateral	The $47.0 billion Treasury and $0.52 billion overnight repo tranche held at BNY Mellon becomes temporarily inaccessible. Circle's remaining components (SIFI deposits $18.56 billion, other bank deposits $11.28 billion, at institutions independent of BNY Mellon) remain accessible. Accessible reserves within the 48-hour window: approximately $29.84 billion. The BNY Mellon-held reserves are temporarily inaccessible, not lost.
Liquidity Runway	Modelled at $2 billion in redemptions over 48 hours (elevated but below panic scenario). Funded from the bank deposit tranche. Remaining accessible reserve: approximately $27.84 billion. Circle can service elevated demand for approximately 15 days before bank deposit reserves are exhausted, well beyond the 48-hour scenario.
Anticipated Investor Actions	Market uncertainty about Circle's ability to honour redemptions; secondary market discount of approximately 0.3% to 1.0%. Institutional holders may pause new purchases pending clarity.
Conclusion	Solvent but gated. Total reserves are fully intact; the constraint is temporary inaccessibility of the BNY Mellon-custodied portion. This scenario is less severe than the SVB-2023 analog (where the affected deposit was approximately $3.3 billion at a single bank), as BNY Mellon is a G-SIB with systemic regulatory backstops and the unaffected reserve portion ($29.84 billion) provides ample 48-hour runway.
Impact	Medium

5.4 Regulatory and Legal Jurisdiction

Issuer jurisdiction: Delaware, USA (primary); France (EU operations)

Governing law: New York State law (per Circle Terms of Service); EU law for USDC issued as an electronic money token under MiCA by Circle Internet Financial Europe SAS

REGULATORY ITEM	DETAIL
Primary regulator	FinCEN (federal, USA); state banking and finance regulators (50 US states and DC); NYDFS (New York); ACPR / Banque de France (EU/France)
Licence / registration	Money Transmitter Licence (all 50 US states and DC); MSB registration (FinCEN); BitLicence (NYDFS); Electronic Money Institution (EMI) licence (ACPR, France, passportable across EEA)
AML / KYC framework	Bank Secrecy Act (BSA) / Patriot Act customer identification (USA); EU Anti-Money Laundering Directives (AMLD6 and successor framework); MiCA Title IV (EU); FATF Travel Rule compliance for institutional transfers above applicable thresholds
Enforcement history	No material regulatory fines or orders against Circle related to USDC issuance or reserve management identified as of the assessment date
Pending proceedings	No known material litigation or regulatory proceedings as of the assessment date

Circle is among the most broadly licensed stablecoin issuers globally. The ACPR EMI licence, obtained in 2024, enables Circle to issue USDC as an electronic money token across the EEA under MiCA, one of the first major stablecoin issuers to achieve MiCA authorisation. In April 2025, the US SEC issued a Statement on Stablecoins concluding that fully-backed payment stablecoins such as USDC do not constitute securities under applicable federal securities laws, removing USDC from SEC registration requirements.

The on-chain blacklisting mechanism (Section 2, KYC Gating) provides the primary protocol-level enforcement channel for OFAC sanctions compliance. Circle has blacklisted hundreds of addresses in response to OFAC designations and law enforcement requests, including Tornado Cash-related addresses in August 2022. The blacklisting mechanism is among the strongest on-chain AML enforcement tools available in the stablecoin space.

Regulatory risk assessment: The most significant regulatory risk for USDC is the enactment of US federal stablecoin legislation. Bills progressing through Congress as of mid-2026 (including the GENIUS Act and competing proposals) would impose federal licensing requirements, enhanced reserve segregation, direct redemption right mandates, and potential limitations on eligible reserve assets. Circle is well-positioned to comply with most proposed frameworks; the regulatory trajectory is broadly supportive of regulated, bank-supervised stablecoin issuers. If enacted with strong bankruptcy-remote requirements, pending legislation would close the current gap in direct holder claims on reserve assets and could improve the financial risk rating.

Under MiCA, ongoing obligations include redemption within one business day at par, reserve asset restrictions (HQLA only), and operational resilience requirements. Circle's current reserve composition is permissible under MiCA rules for significant EMTs. If USDC is designated as a significant EMT, enhanced EBA supervision applies.

The legal nature of USDC holder claims is the primary residual regulatory risk: holders have a contractual redemption right against Circle, not a direct legal claim on specific reserve assets. In a Circle insolvency, holders would likely be unsecured creditors under current US law, subject to applicable state insolvency proceedings. The concentration of issuer risk on Circle as the sole post-2023 issuer (after dissolution of the Centre Consortium) amplifies this point.

6. Conclusion

6.1 Composite Risk Rating: Low

Composite Confidence: Low

DOMAIN	RISK RATING	CONFIDENCE
Smart Contract Security	Low	High
Operational Security	Medium	Low
Financial Integrity	Low	Medium

The composite risk rating is **Low**, derived from the three domain ratings: two Low (smart contract security, financial integrity) and one Medium (operational security). The Medium operational security condition reflects the concentration of the highest-privilege roles (proxy admin and implementation owner) in EOAs with no publicly disclosed key management arrangements, and the absence of any on-chain timelock or second-approval requirement for upgrades or role reassignments. This condition is calibrated as Medium rather than High because no known key compromise, unauthorised minting, malicious upgrade, or operational control failure has been identified in USDC's history, and the operational risk is contingent rather than actively causing holder harm. At most one domain reaches Medium, and the Medium condition is future-oriented (it concerns what would happen if a key were compromised, not an active compromise): this places the composite at **Low** per the rating standard.

Composite confidence is **Low**. Smart contract confidence is High: formal verification returned CONFIRMED results for all four hidden-surface cases (proxy routing to fixed implementation confirmed; unknown selectors and short calldata always revert at the implementation), and fork-based behavioral tests passed 64/64 required cases. Financial confidence is Medium because cross-chain supply data and some banking counterparty identities are not independently verified. Operational security confidence is Low because the highest-privilege roles are EOAs with immediate upgrade and role-reassignment authority, and the report lacks independently verifiable evidence for HSM/MPC custody, second approval, emergency procedure, monitoring thresholds, or change-control workflow. This Low-confidence operational domain is material to the composite conclusion and prevents the composite confidence from rising above Low.

6.2 Improvement Suggestions

- **Operational transparency disclosure:** Circle does not publicly disclose the key management policy for its on-chain privileged role holders (proxy admin, implementation owner, MinterAdmin owner, blacklister, pauser), its recovery and incident response playbook for privileged contract roles (covering key loss, key compromise, and emergency contract intervention scenarios), or its monitoring policy for on-chain

privileged events (mints, burns, role changes, upgrades, pauses, and associated detection thresholds). Publishing these three disclosures would allow independent verification of operational controls, improve confidence in the operational security domain, and represent meaningful transparency for USDC holders at scale. Disclosure of the banking counterparties for the "other bank deposits" reserve tranche would similarly improve financial confidence.

6.3 Report Validity Timeline

This report is valid as of its publication date. It should be treated as superseded upon any of the following events, whichever occurs first:

- A smart contract upgrade that modifies the in-scope bytecode at `0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48` (proxy) or `0x43506849D7C04F9138D1A2050bbF3A0c054402dd` (implementation)
- A change to any privileged role holder identified in Section 4.1
- A material change to the custodian, redemption model, or reserve composition identified in Sections 5.1 and 5.4
- 12 months from the date of publication

DISCLAIMER